ALAN CHARLES RAUL

Comments of Alan Charles Raul. These comments do not necessarily reflect the views of Sidley Austin LLP or any of its clients.

1. The Department of Commerce Should Promote Harmonization, Coordination, and Streamlining of Privacy, Security and Consumer Protection in the United States and Internationally in Order to Achieve a High Level of Substantive Privacy Protection Without Imposing Needless Burdens; and Commerce Should Ensure that the Costs and Benefits of Privacy Regulation Are Consistently and Fairly Evaluated.

There is a prevailing sense today that existing privacy and data security standards are more complicated, conflicting and onerous than necessary or appropriate in order to achieve a high substantive level of personal protection. There are so many international, federal, state, local and private standard-setters striving to achieve fairly comparable substantive objectives that the transaction costs of compliance are not always producing commensurate benefits for society. Moreover, while territorial jurisdiction, and separate regulation for separate political communities, continue to be immensely germane even as the world flattens, it is indisputably true that the flow of data and deployment of innovations in the information-based economy are inherently less territorial than other elements of international trade, commerce, finance, manufacturing or agriculture.

More effective coordination of privacy, data security and trade practice regulation could foster greater certainty, predictability and innovation – and substantive protections – benefiting both businesses and consumers involved in the Internet economy. Today, there is too much counter-productive conflict – or perceived conflict – between the rules of different states, agencies, countries and multilateral institutions.

In view of the relatively substantial degree of agreement over fundamental principles and fair information practices, the conflict of regulatory standards is pure friction – it imposes a drag on the economy in terms of excessive compliance costs and citizen confusion without necessarily achieving meaningful additional benefits in privacy, security or consumer protection.

The Department of Commerce should thus ensure that data protection regulations are analyzed under Executive Order 12866 to assess whether

the costs and benefits (including intangible benefits) are properly and reasonably aligned. This process should also cover privacy and data security regulations issued or administered by agencies that are not directly accountable to the President, such as the Federal Trade Commission, Federal Communications Commission, Securities and Exchange Commission, etc. The American people are entitled to privacy and security regulations that are substantively protective and cost-effective (taking into account relevant non-pecuniary harms where appropriate). Regulation that has not been submitted to cost-benefit analysis will surely not be as beneficial or efficient as regulation that does pass through this salutary process. To the extent that independent agencies are not formally covered by or subject to Executive Order 12866, the Commerce Department should encourage such agencies to submit to such review and inter-agency comment as a matter of good government and sound administration.

The Department of Commerce should therefore exercise a leadership role within the United States, perhaps in tandem with the Office of Management and Budget, to help harmonize, or coordinate, and streamline the conflicting standards at play throughout the federal government (banking agencies, HHS, FCC, FTC, etc.), state governments and international regulators. Such harmonization or coordination could perhaps be advanced internationally through the Transatlantic Economic Council with the EU, or through parallel activity at the OECD or similar multilateral institutions.

The Department of Commerce, together with the Office of the U.S. Trade Representative, should also ensure that impediments to the flow of personal information and other data do not constitute barriers to international trade that can thwart digital innovation and efficiencies that benefit the economy of the United States, employment and consumer welfare. To the extent, that foreign barriers to information cannot be justified in accordance with legitimate policy objectives to advance substantive privacy rights and protection, those barriers should be challenged under available international agreements.

The Department of Commerce should seek to advance an international approach to the cost-benefit evaluation of privacy and security regulations that could be fairly and reasonably applied to improve different regulatory approaches around the world.

Domestically, Commerce should consider convening councils of interested parties throughout the U.S. including businesses, state attorney generals, consumer regulators, insurance commissioners, etc., to help elaborate best practices and narrow perceived differences in applicable substantive standards for privacy, data protection and Cybersecurity. Specifically, Commerce should determine whether the state-by-state standards for privacy and data security adopted in (e.g.) Massachusetts, California, and elsewhere help advance or impede a robust national digital economy.

In short, the extraterritorial effects of a jurisdiction's regulation of digital and electronic information should be the subject of the Department of Commerce's attention.

Such consideration should take account of the insightful analysis set forth by Judge Loretta A. Preska in American Library Association v. Pataki, 969 F. Supp. 160 (S.D. N.Y. 1997), under the heading of "Federalism and the Internet: The Commerce Clause." Judge Preska wrote:

> The borderless world of the Internet raises profound questions concerning the relationship among the several states and the relationship of the federal government to each state, questions that go to the heart of "our federalism." . . . .
>
> The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation -- and in particular, the national infrastructure of communications and trade -- as a whole.
>
> The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in *Gibbons v. Ogden,* recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to

> term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce. Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.
>
> . . . . Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether.

2. <u>The Commerce Department Should Advocate Internationally on Behalf of the Adequacy of the U.S. Data Protection Regime</u>

As is well known among privacy experts and multinational companies, the EU has not deemed the U.S. regime for privacy and data protection to be adequate, and the E.U. presumably considers the U.S. regime not to be substantially equivalent to that of the EU and its member states. This judgment by the EU results in the imposition of significant hurdles to the efficient management of human resource and customer data within global corporations. Personal data emanating from an organization's EU locations cannot be shared with the same organization's U.S. locations unless certain specific compliance mechanisms are put into place. While most large entities have managed to cope successfully with the demands of the E.U., the necessity of U.S. companies being compelled to do so should be addressed by the Commerce Department.

Given the numerous privacy laws and regulations, and general unfair and deceptive trade practice statutes, enforced by the banking and financial regulatory agencies, the Federal Trade Commission, the Federal Communications Commission, the Department of Health and Human Services, the Department of Education, state attorneys general, state insurance commissions, private plaintiffs, the Payment Card Industry and a vigorous advocacy community, it cannot reasonably be argued that the United States has a lower level of data protection than any jurisdiction in the world. Indeed, a strong case can and should be made that the U.S. data protection regime leads the world in both substantive rigor and

practical flexibility -- especially with regard to particularly sensitive categories of personal information such as financial, medical or communications data (each of which is subject to specific Acts of Congress and dedicated, sectoral regulation).

The United States has also plainly led the way internationally with regard to data security, where data breach notification and affirmative information security requirements are now well entrenched in U.S. law and practice.

Accordingly, Commerce should consider advocating that the E.U. determine without further delay that the U.S. system for protecting personal privacy and information security is at least as stringent as that of the E.U. To the extent that the E.U. can identify any specific areas of data collection or use where the U.S. system does not adequately protect the regulatory interests of E.U. citizens, those specific, limited circumstances could be addressed separately with special protections or limitations, rather than bogging down the entire international flow of data across the Atlantic.

The Commerce Department, with the Department of Justice and the Securities and Exchange Commission, should also play a role in ameliorating international disputes over civil discovery, internal investigations, and compliance with U.S. corporate laws. While it must be acknowledged that certain other countries object to the substantive policies underlying discovery in U.S. civil litigation and the obligations of U.S. companies to ferret out violations of the Foreign Corrupt Practices Act and other corporate malfeasance, Commerce should help lead an effort to diminish the considerable tensions and conflicts faced by U.S. companies that strive to comply simultaneously with legal obligations in all of the numerous jurisdictions in which they operate.

3. <u>The Greatest Threats to Personal and Proprietary Information Today Arise in the Realm of Cybercrimes and Breaches of Cybersecurity Perpetrated by Sophisticated Criminals and Hostile State-Supported Actors; Commerce Should Facilitate Collaboration Between the Public and Private Sectors and Help Reconcile the Resources Allocated to Cybersecurity with Those Allocated to Basic Information Security and Data Breaches.</u>

The Department of Commerce, working with White House, OMB, the Office of the Director of National Intelligence, the Department of Homeland

Security and the Cyber Command in the Department of Defense could help mediate the necessary collaboration between the federal government and the private sector to ensure that the requisite knowledge and resources are shared with private companies to help protect personal information, critical information infrastructures, and important intellectual property and proprietary information against aggressive exploitation by sophisticated cybercriminals.

The risk of such cyber attacks has been identified as a leading threat to the national security and economic well being of the United States. The Department of Commerce should play a role in ensuring that concerns over marketing uses of personal information by legitimate businesses do not overwhelm attention to the greater risks of cyber attacks and cybercrimes by avowedly hostile and criminal enterprises.

4. Commerce Should Ensure that the Benefits of the "Notice and Choice" Paradigm – Namely, Allowing Considerable Freedom of Contract, Flexibility and Innovation – Are Preserved Even as Additional Privacy Regulations Are Being Considered by Other Federal, State and International Regulators.

There has been considerable consternation over whether the current "notice and choice" paradigm, which requires companies that collect information about consumers to provide notice about their data practices and obtain the express or implied consent of their consumers to those practices, is working well enough to protect consumers' privacy interests. In particular, concern as been expressed whether any consumers actually read and understand the privacy polices that are intended to convey such notice and effectuate such consent.

While addressing such concerns can and should be the subject of extensive comments and deliberation, the Commerce Department should take note of the fact that there is an extensive community of privacy advocates that routinely scrutinizes privacy policies and often raises (effective) objections when such policies are perceived to over-reach. While the content of privacy policies, and the interaction of such policies and affected consumers, can no doubt be considerably enhanced, there is little reason to thoroughly abandon a paradigm that the federal government has itself championed in legislation, regulation and enforcement, and which allows companies to innovate and communicate relatively flexibly.